AN OIG GUIDE FOR LSC-FUNDED PROGRAMS

"How to Prevent Computer Laptop Theft or Loss"

- ***Laptop Theft and Loss Is a Serious Problem***
  - Laptop theft and loss is the most frequently reported loss by LSC grantees
    - Even the FBI reportedly loses 3-4 laptop computers each month and they are unable to say in many instances whether information on the machines is sensitive or classified[1]
- ***Laptop Theft and Loss Is a Serious Risk***
  - A laptop can be very expensive to replace
    - Replacing software and lost information costs even more
  - Laptops often contain sensitive client and personal information
    - Information from a stolen laptop can place clients at risk by revealing confidential and privileged information and also could result in identity theft
  - The theft or loss of a laptop disrupts and adversely affects work product and output
  - Program management is responsible for assessing risk and establishing adequate controls to prevent loss or theft[2]

[1] http://tig.lsc.gov/TIG/Holly_Rosslsc_security.ppt#274,1,Security Matters

[2] In the past, OIG has reported that the cost of laptop computers does not always meet the dollar threshold for controlling more expensive capital assets, laptop computers can contain sensitive information, easily be put to personal use, and can cause a considerable burden on an organization when they need to be replaced. Controlling sensitive assets like laptop computers ensures that assets are adequately protected, increases the probability of recovering lost or stolen items, and reduces overall operating costs. Grantee management should review all assets and determine which assets should be controlled. https://www.oig.lsc.gov/reports/0802/au08-02%20Laurel%20Legal%20Services.pdf

"How to Prevent Computer Laptop Theft or Loss"

- ***Adequate Steps Should Be Taken to Prevent Theft or Loss***

  - Make sure you record the make, model and serial number of the laptop and store this information in a secure place

  - Never leave a laptop in an unlocked vehicle, even if the car is in your driveway; lock it in the trunk if it needs to be left in a car

  - Keep laptops in carry-on bags while flying to avoid loss or damage as checked baggage

  - When going through security screening keep an eye on your laptop

  - At hotels lock your laptop in a safe place if possible

  - Secure shared laptops in a central location when not in use[3]

  - Do not leave laptops unattended in places like unlocked conference rooms

  - Restrict unauthorized access to the office to deter laptop theft

  - Install software that tracks your laptop if stolen or lost

  - Back up confidential information in case the laptop is lost or stolen on a thumb drive or other detachable device

  - Regularly purge unneeded data files from your laptop

  - Store all data on the server, not laptops, and use the laptop as a "dummy" terminal

  - Install encryption software to protect sensitive information

[3] On several occasions the grantee did not know when the laptop was stolen because it had been checked out to be used for presentations and the theft was not discovered until someone else wanted to use it.

"How to Prevent Computer Laptop Theft or Loss"

- ***Laptop Theft Should Be Reported***
  - Promptly report thefts to the local authorities and LSC-OIG
  - Make sure you have the make, model and serial number available so police can file a complete report and enter the stolen laptop information immediately on the national crime information database
  - If the laptop is stolen and contains confidential information, assess whether you need to contact your clients or other persons about the loss

- ***Please Remember to Contact the OIG***
  - Pursuant to LSC Grant Assurances, grantees must promptly contact the Office of Inspector General (OIG) about embezzlements and other thefts
  - OIG has investigators and auditors on staff with considerable expertise in preventing, detecting, and investigating fraud
  - Please remind your employees about the OIG Hotline at (800) 678-8868 or (202) 295-1670, email hotline@oig.lsc.gov or mail to P.O. Box 3699, Washington, DC 20027-0199
  - Complainants' names will remain confidential, if desired
  - You may also contact:
    - Mike Shiohama, Chief Investigator, by telephone at (202) 295-1655 or by email at ms@oig.lsc.gov
    - Tom Coogan, Assistant Inspector General for Investigations, by telephone at (202) 295-1651 or by email at tc@oig.lsc.gov

April 2009